

09841700-00214360

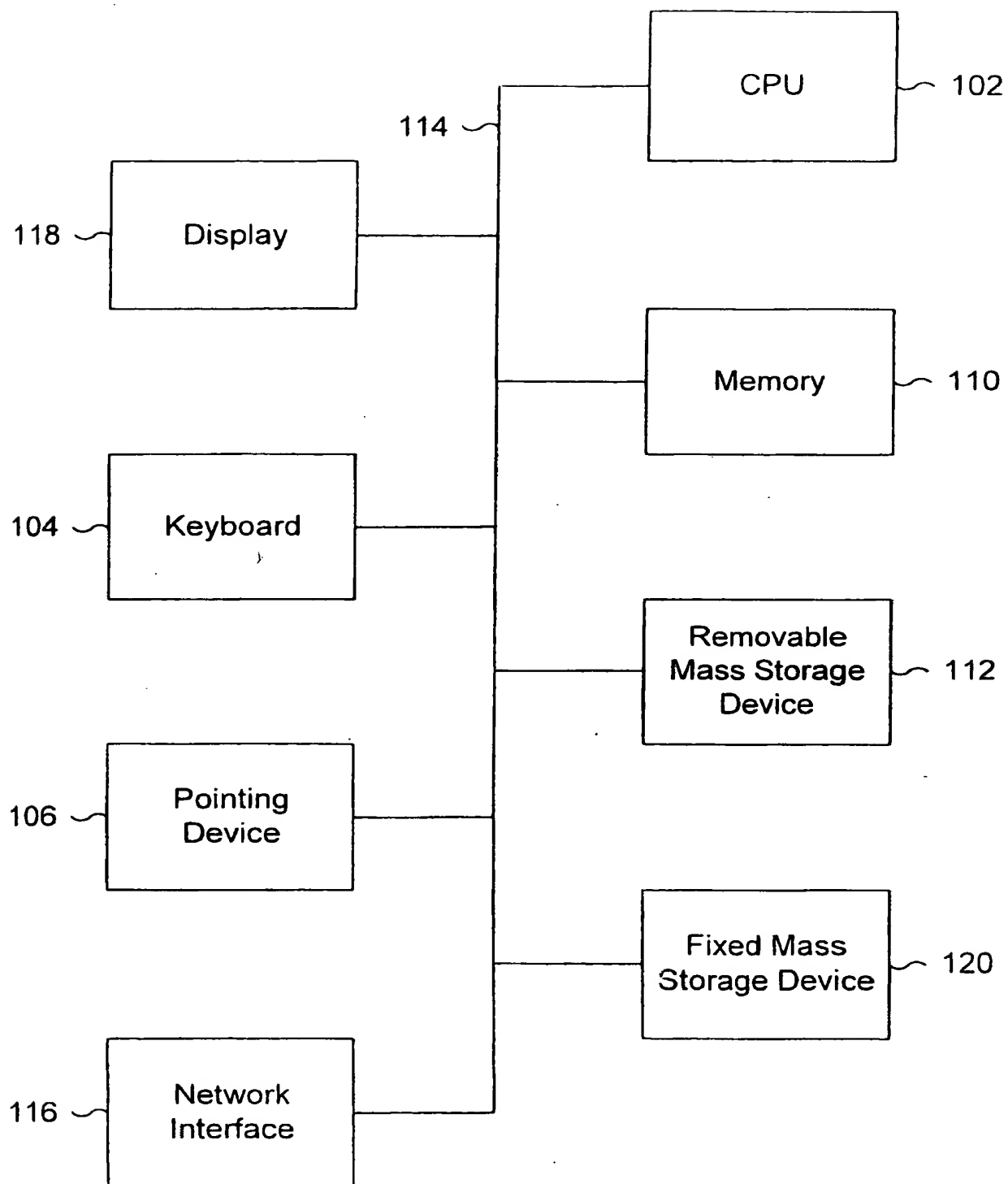


Figure 1

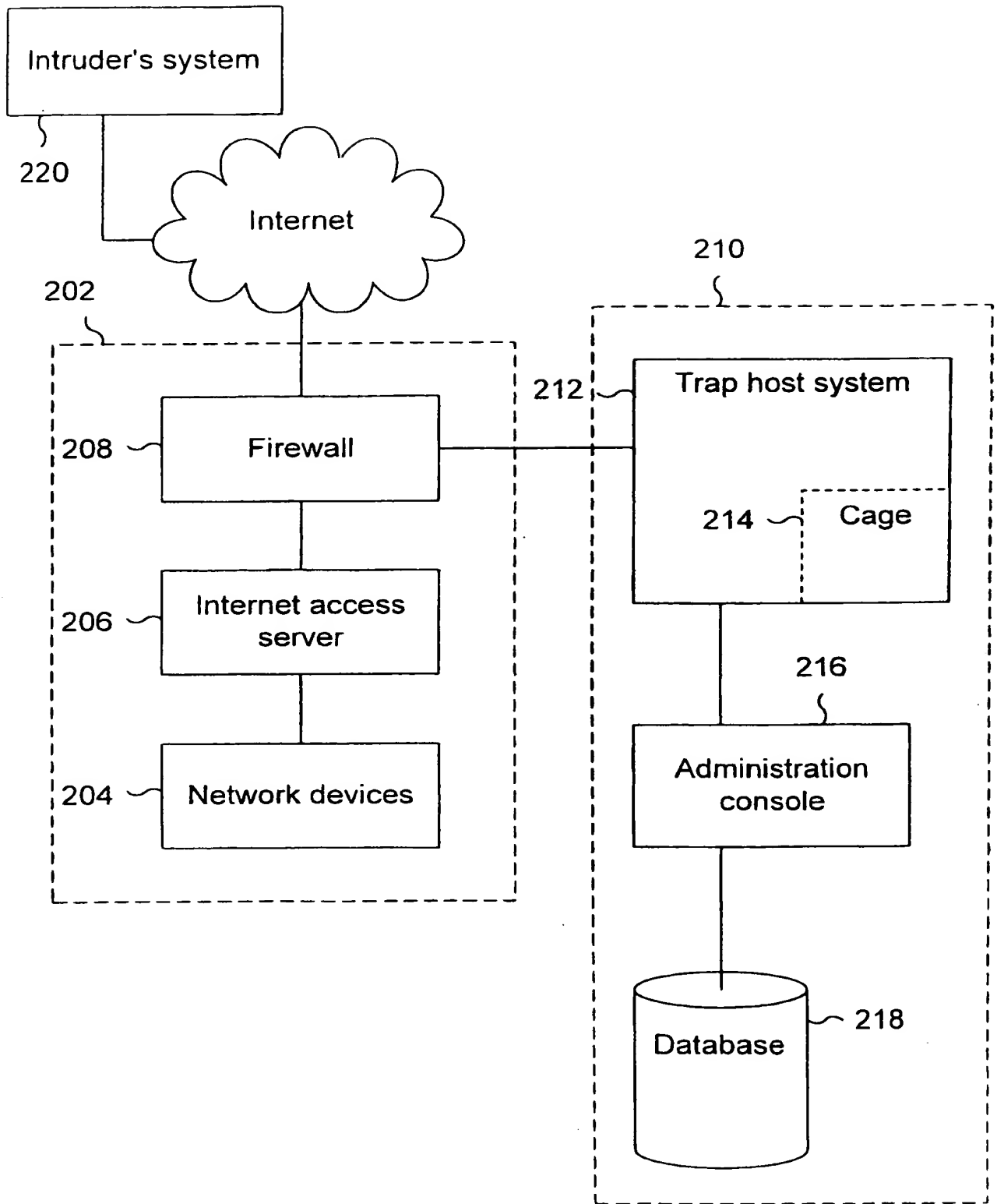


Figure 2

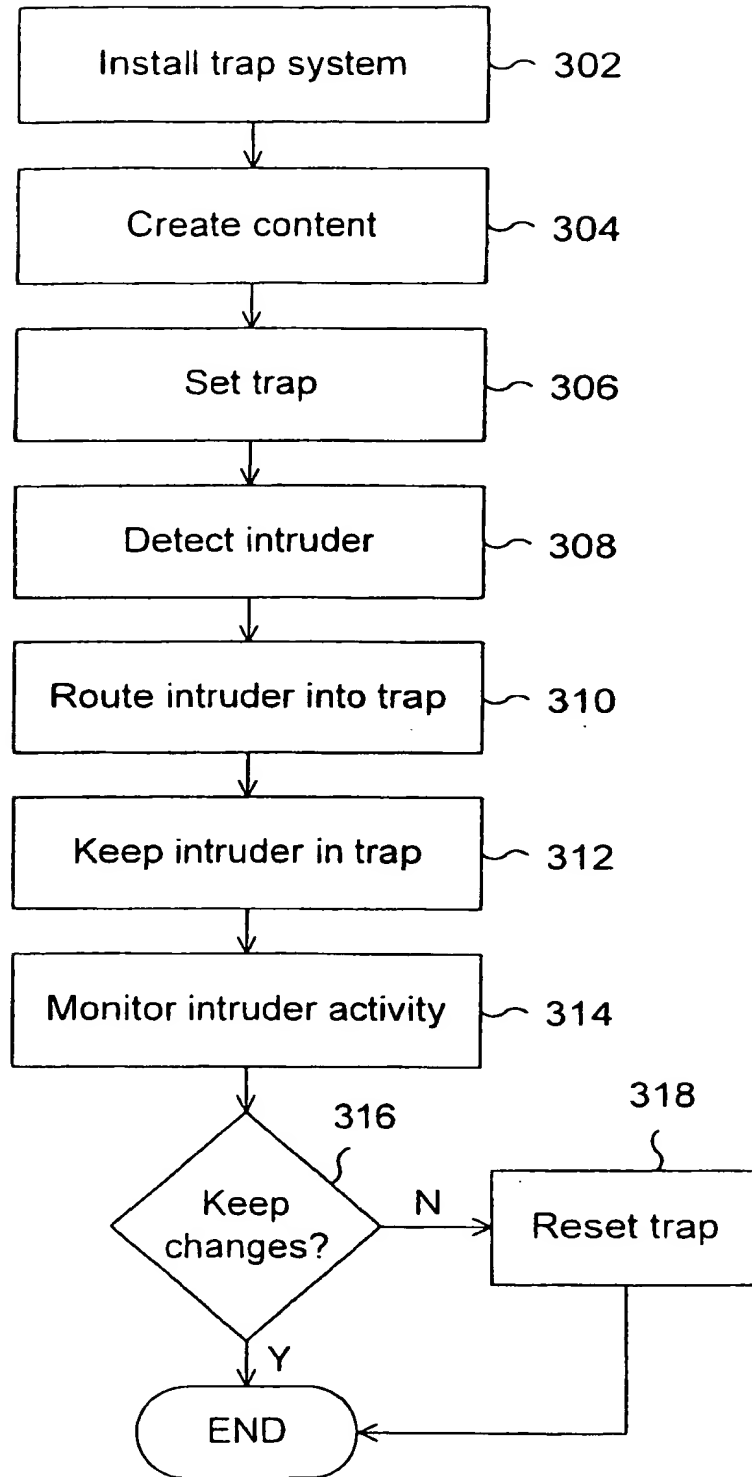


Figure 3

09441700:072704

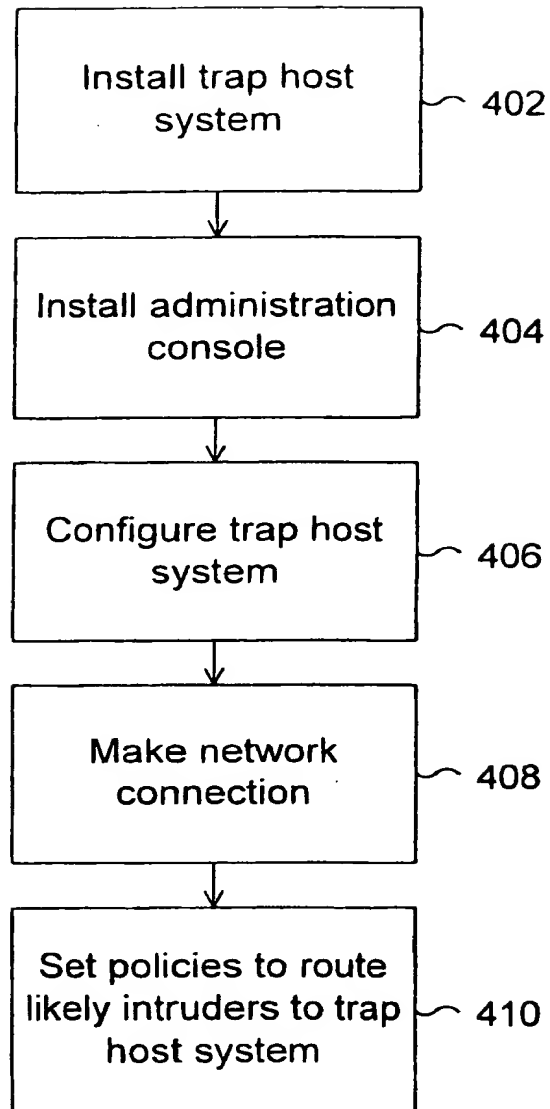


Figure 4

104220-00274350

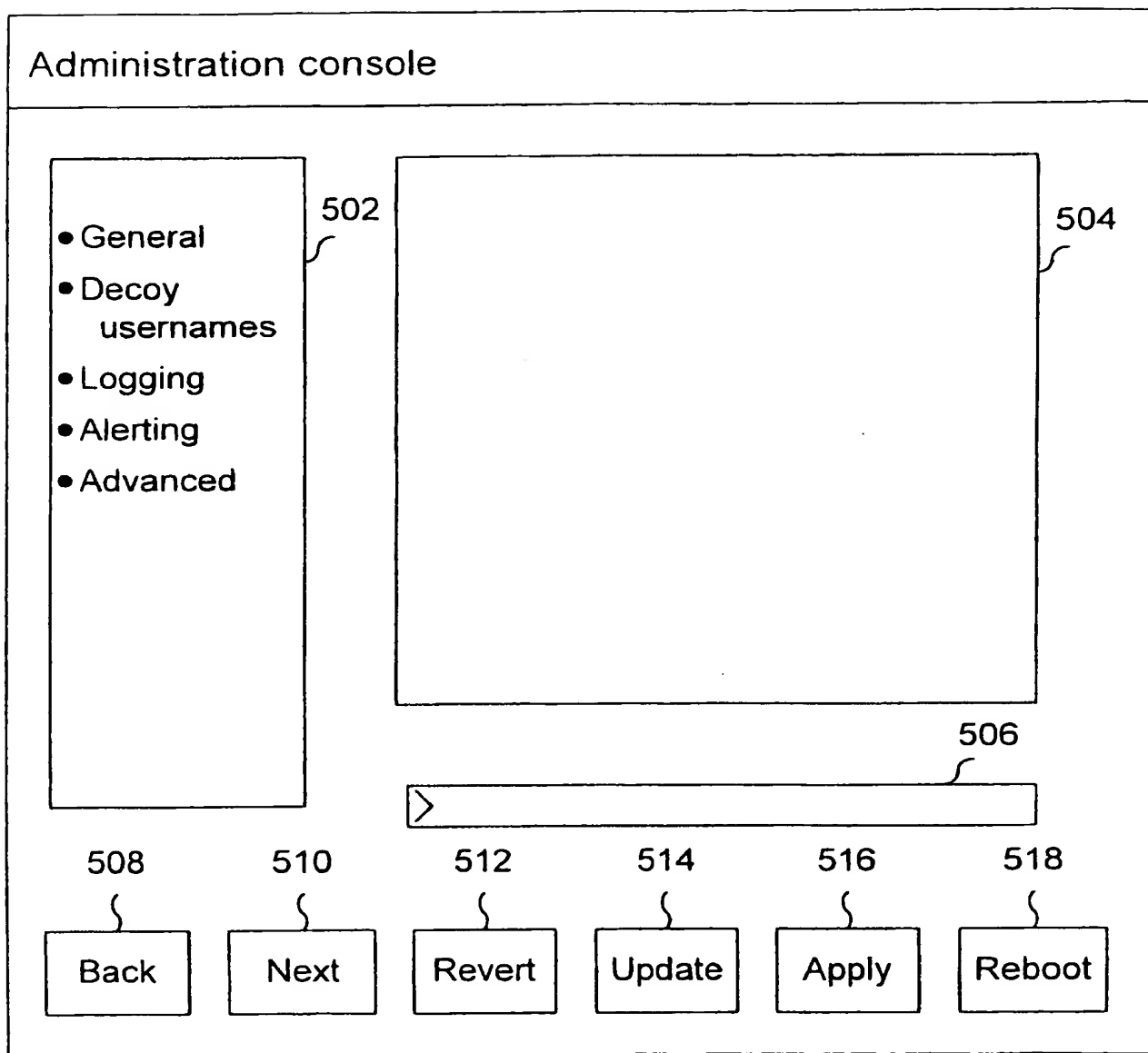


Figure 5

09641700-02201

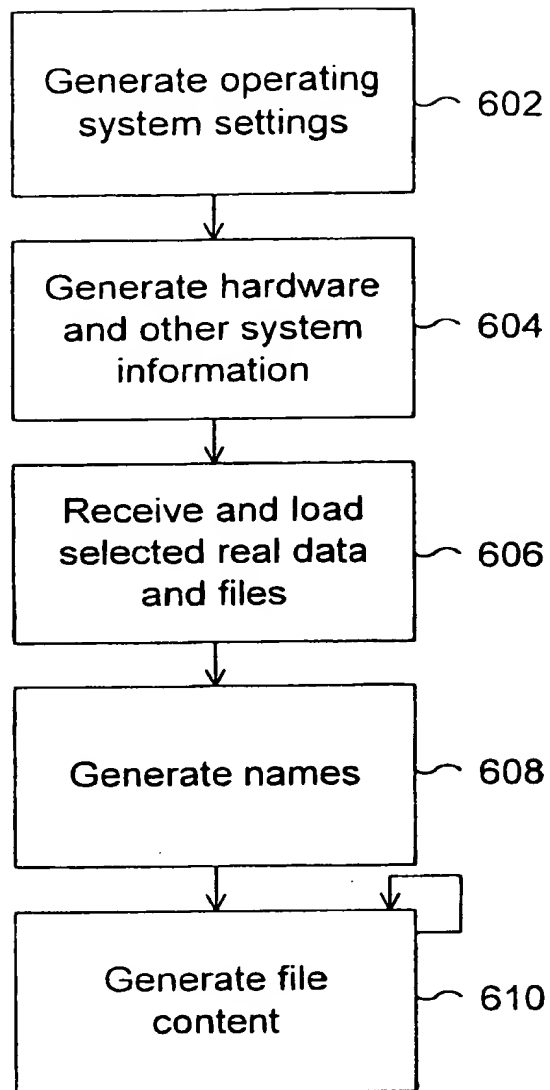


Figure 6

09841300.07201

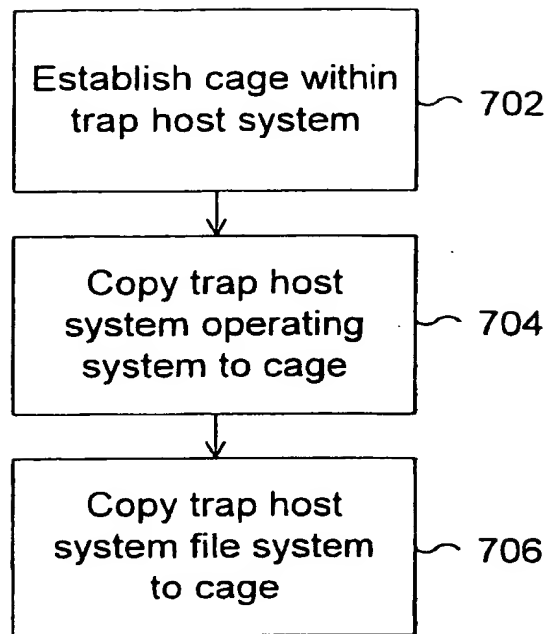


Figure 7

0984100:072701

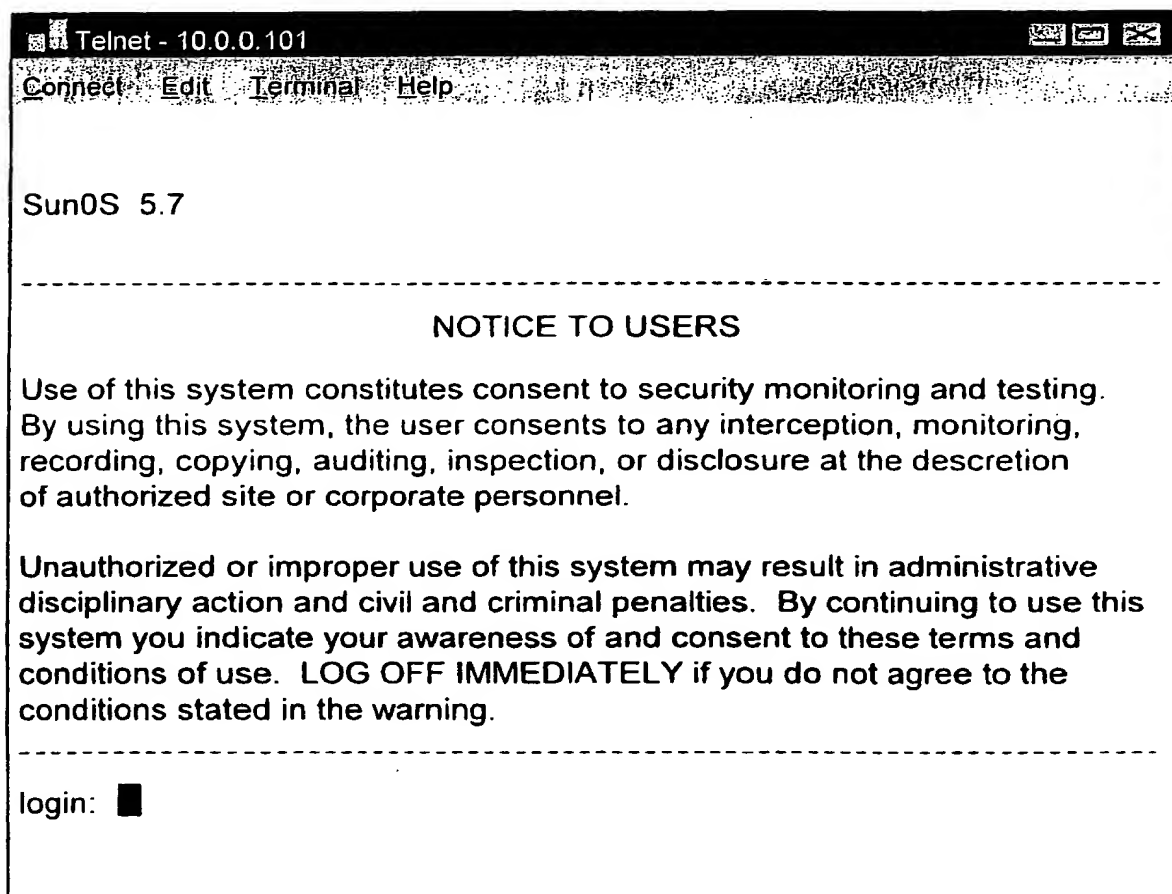


Figure 8



09841700:072701

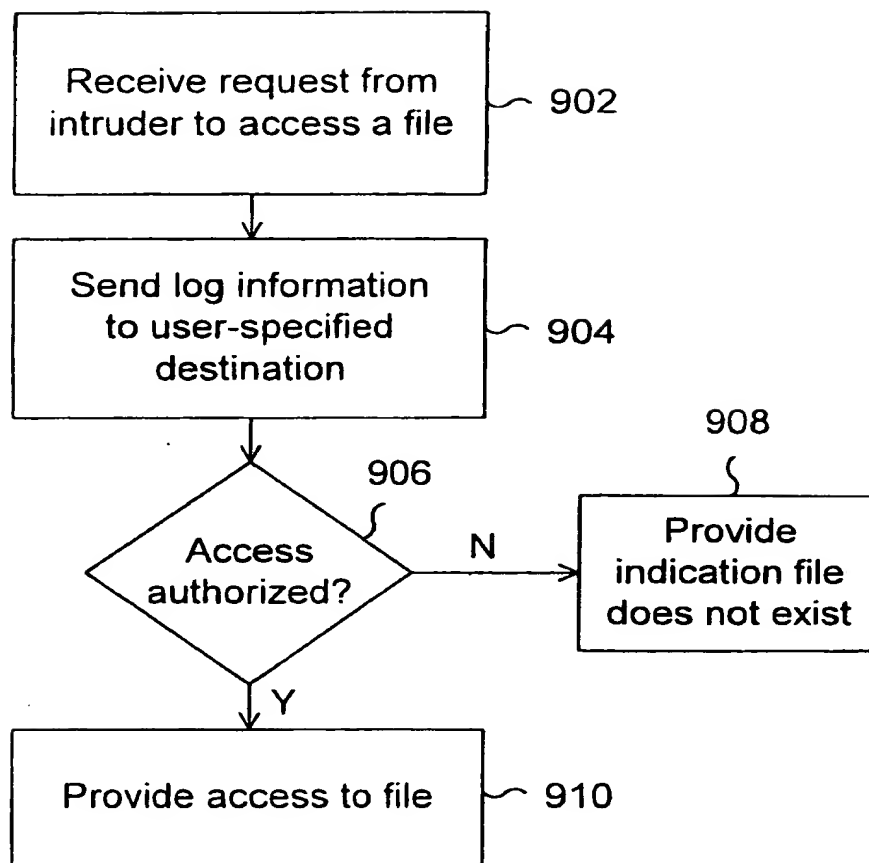


Figure 9

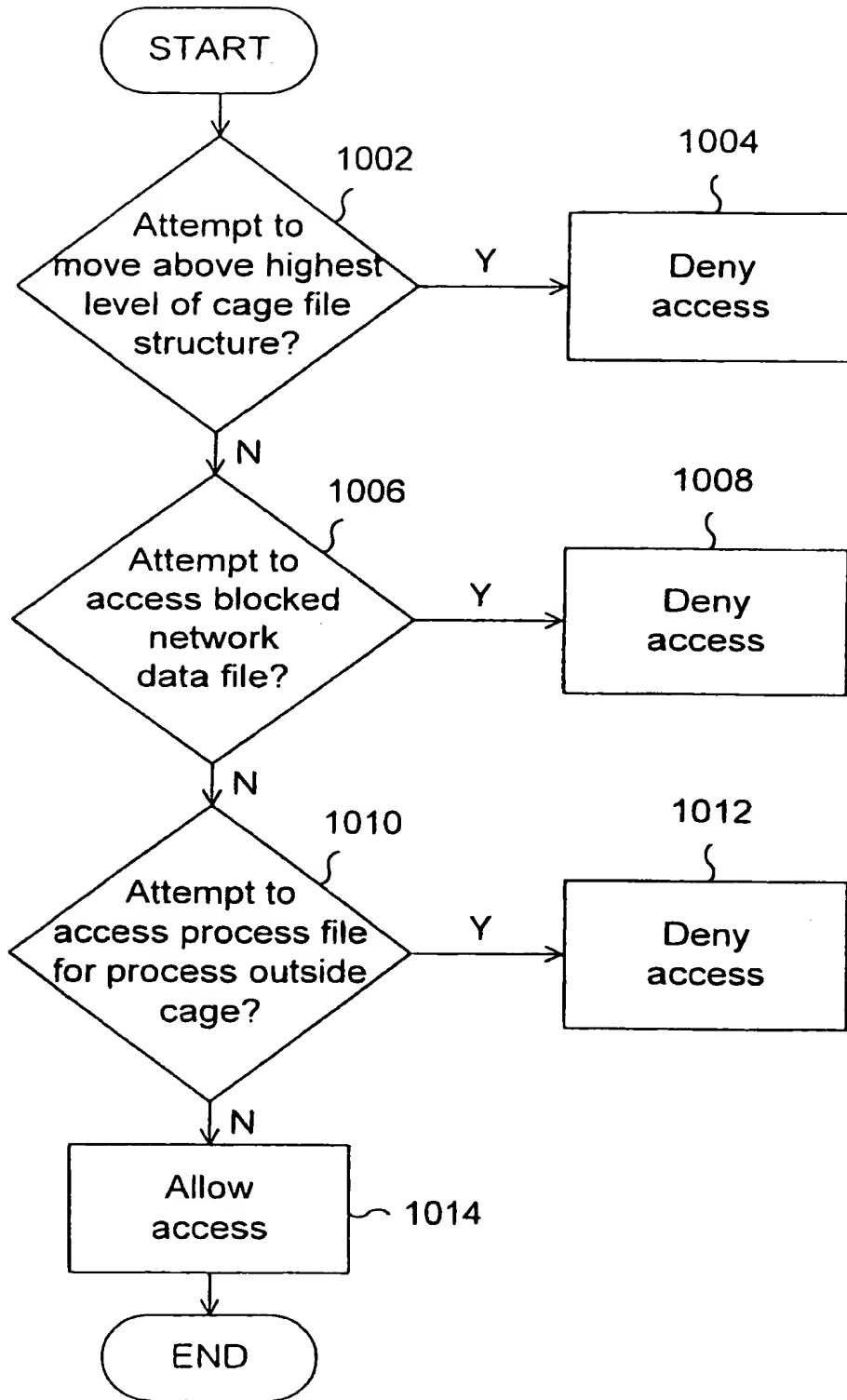


Figure 10

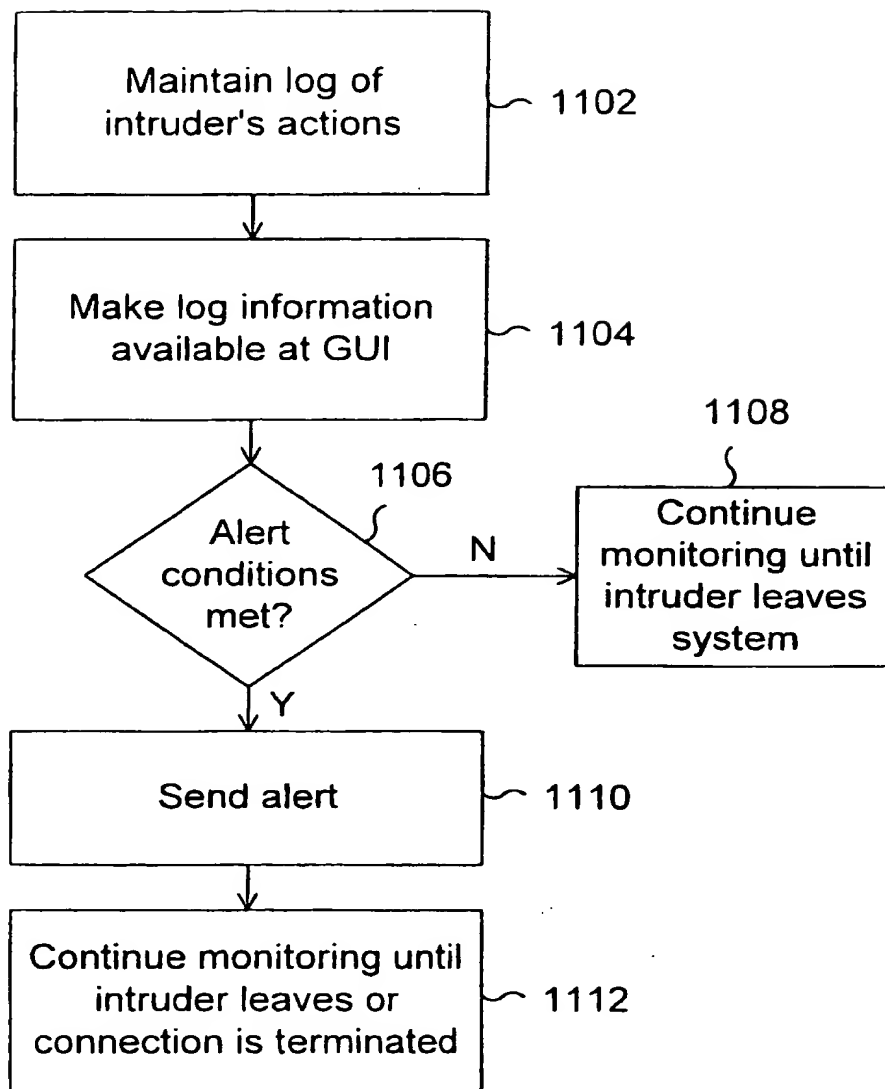


Figure 11A

0941700.0741360

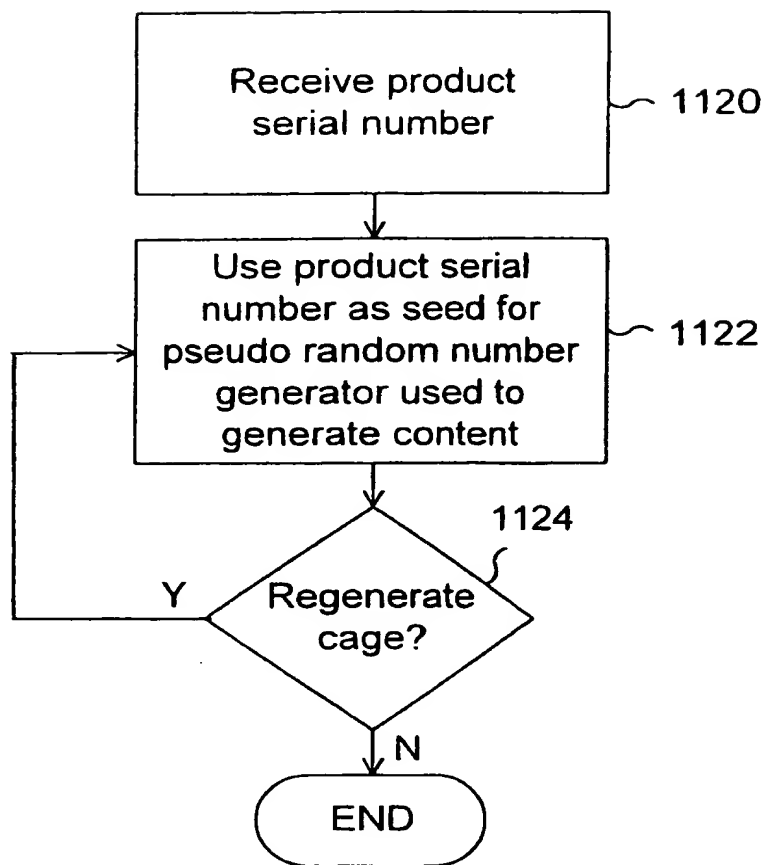


Figure 11B

09441700 02701

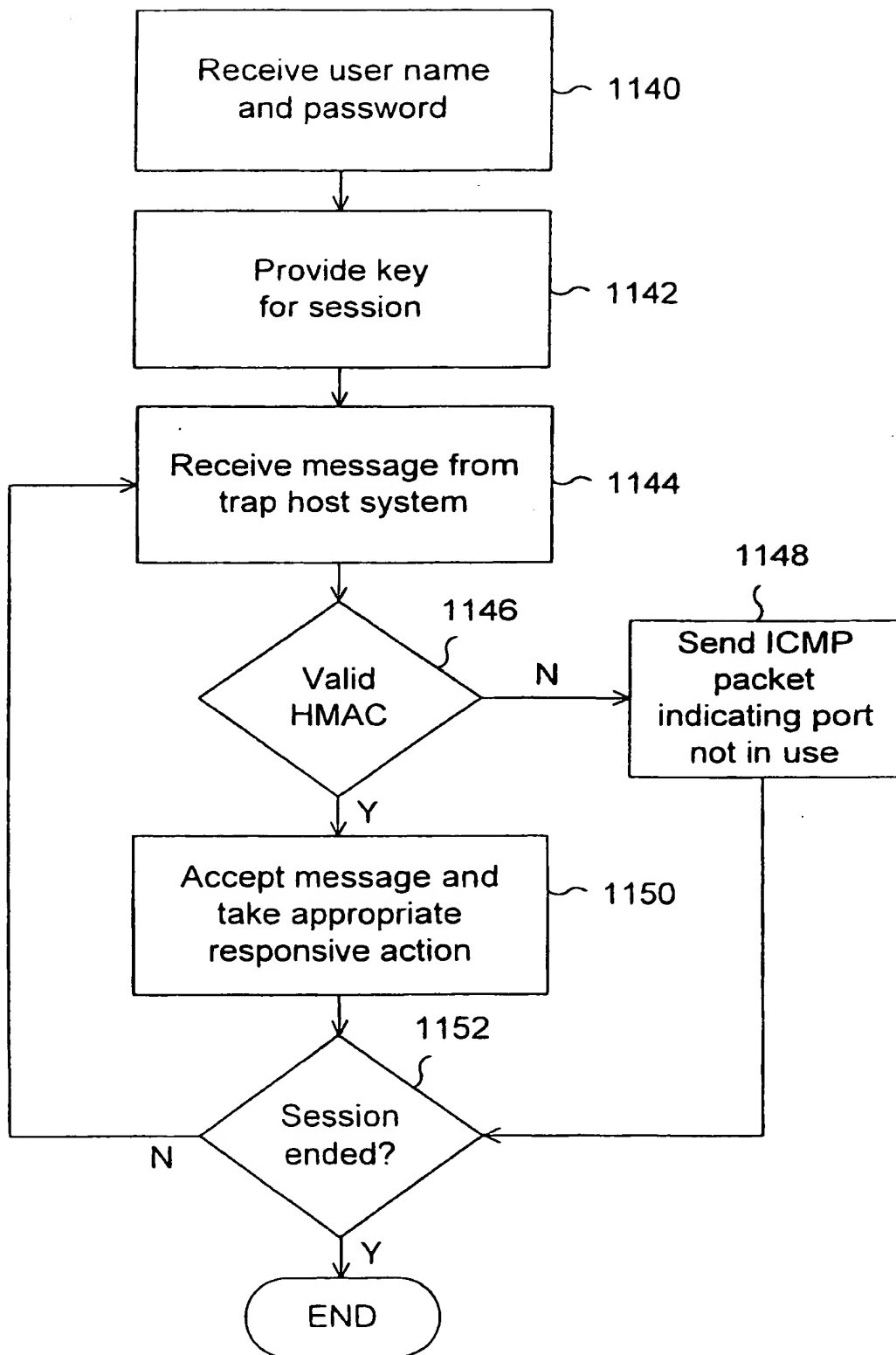


Figure 11C

09341700-072701

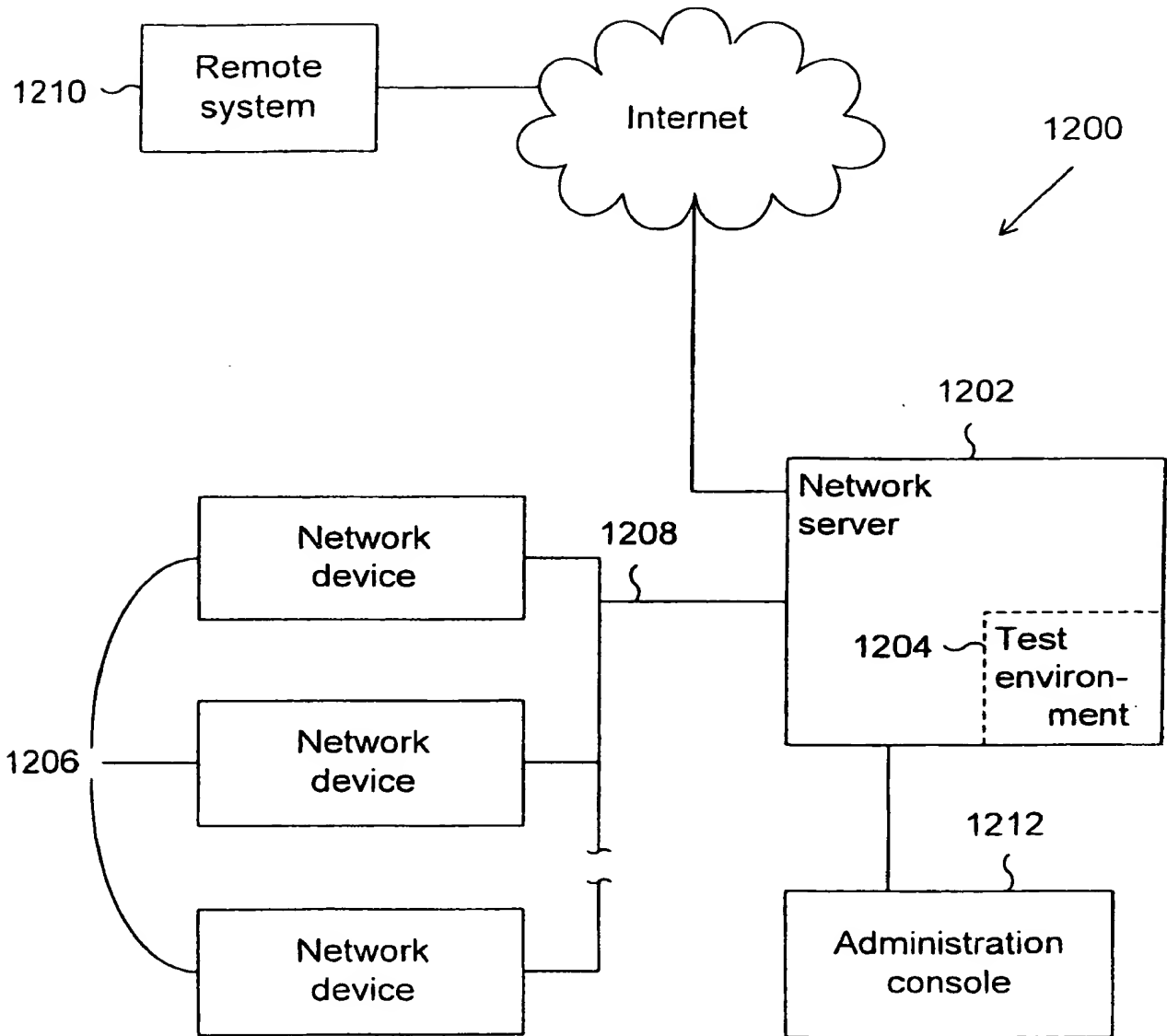


Figure 12

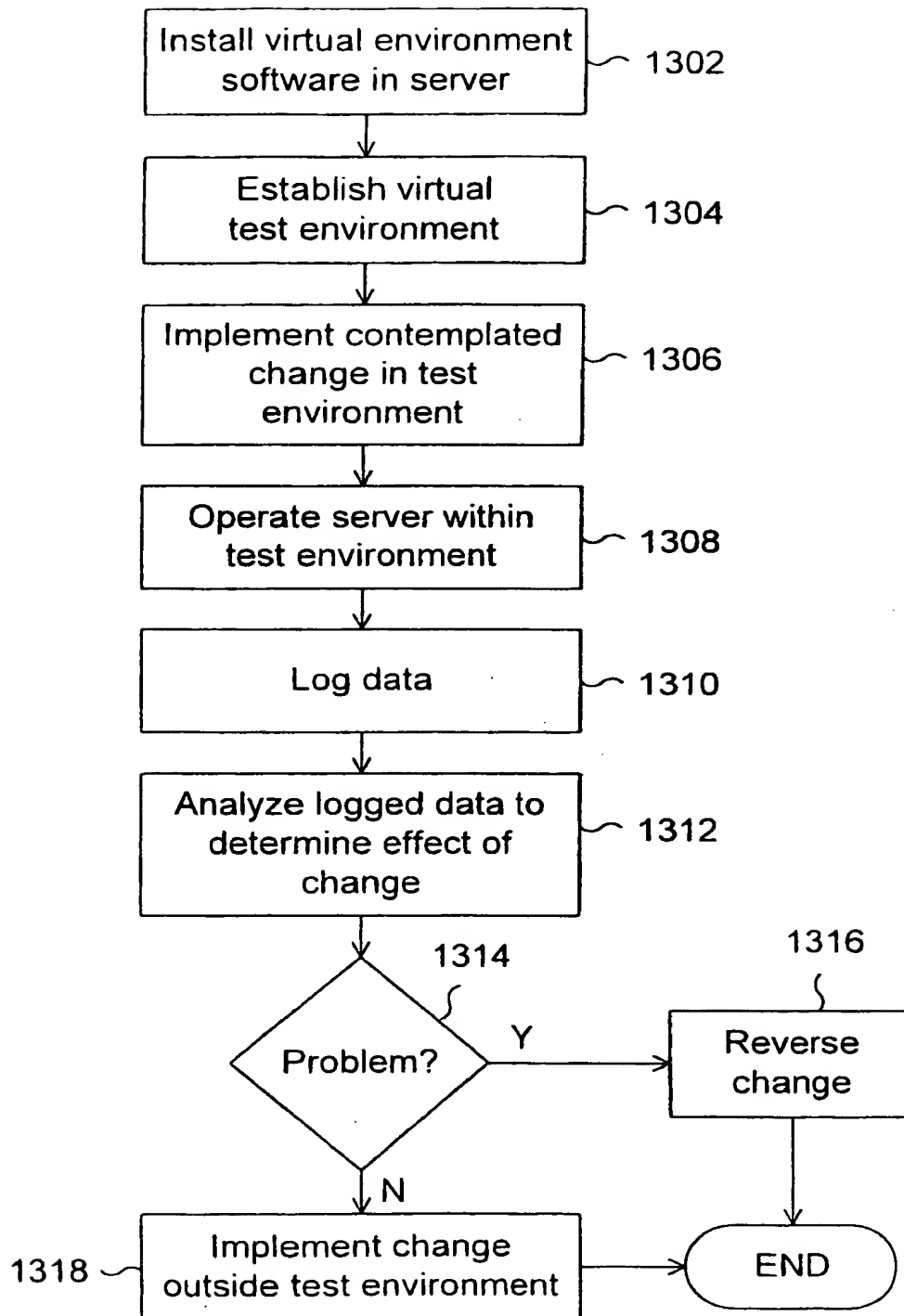
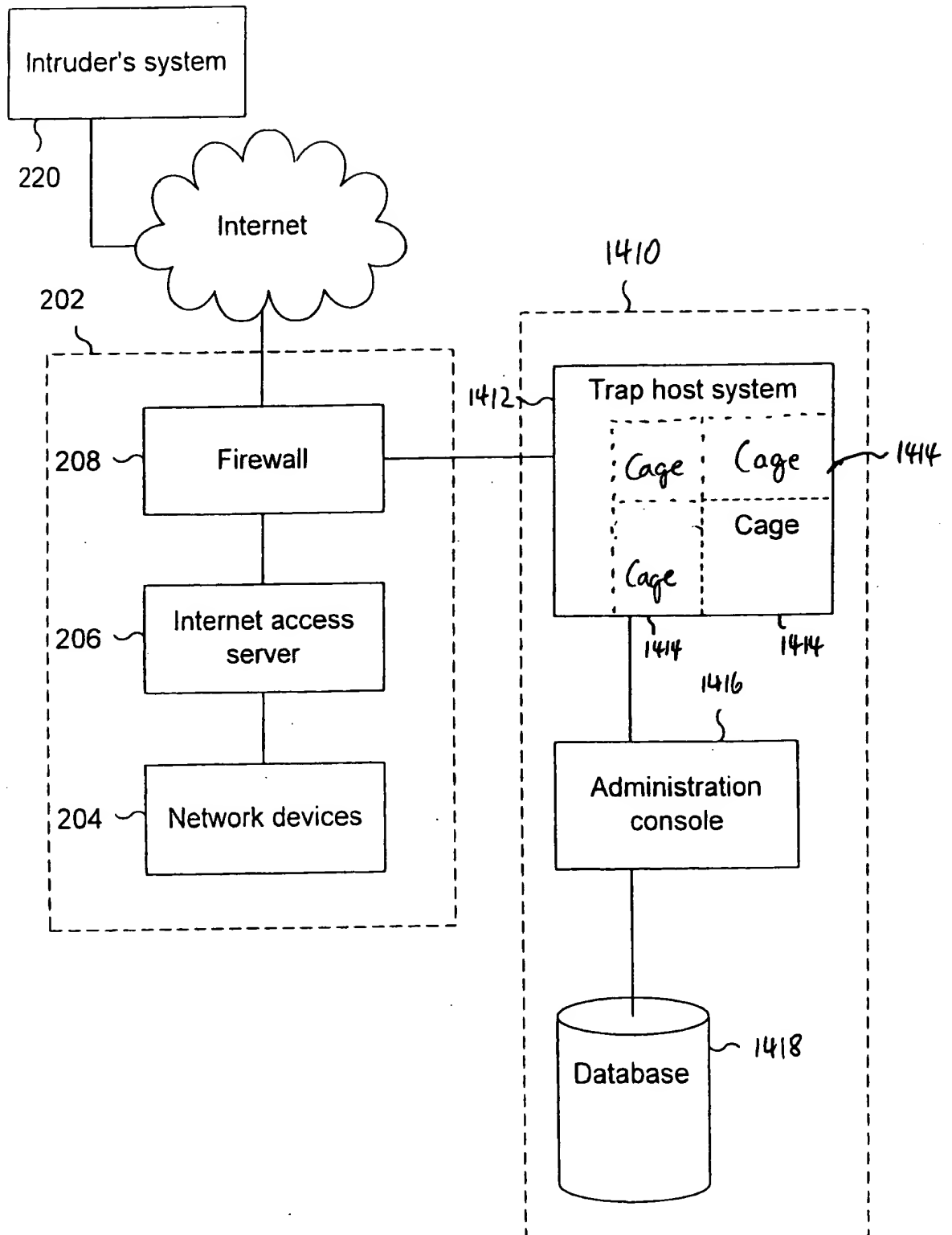


Figure 13

0941700:0274360





0844700:072701

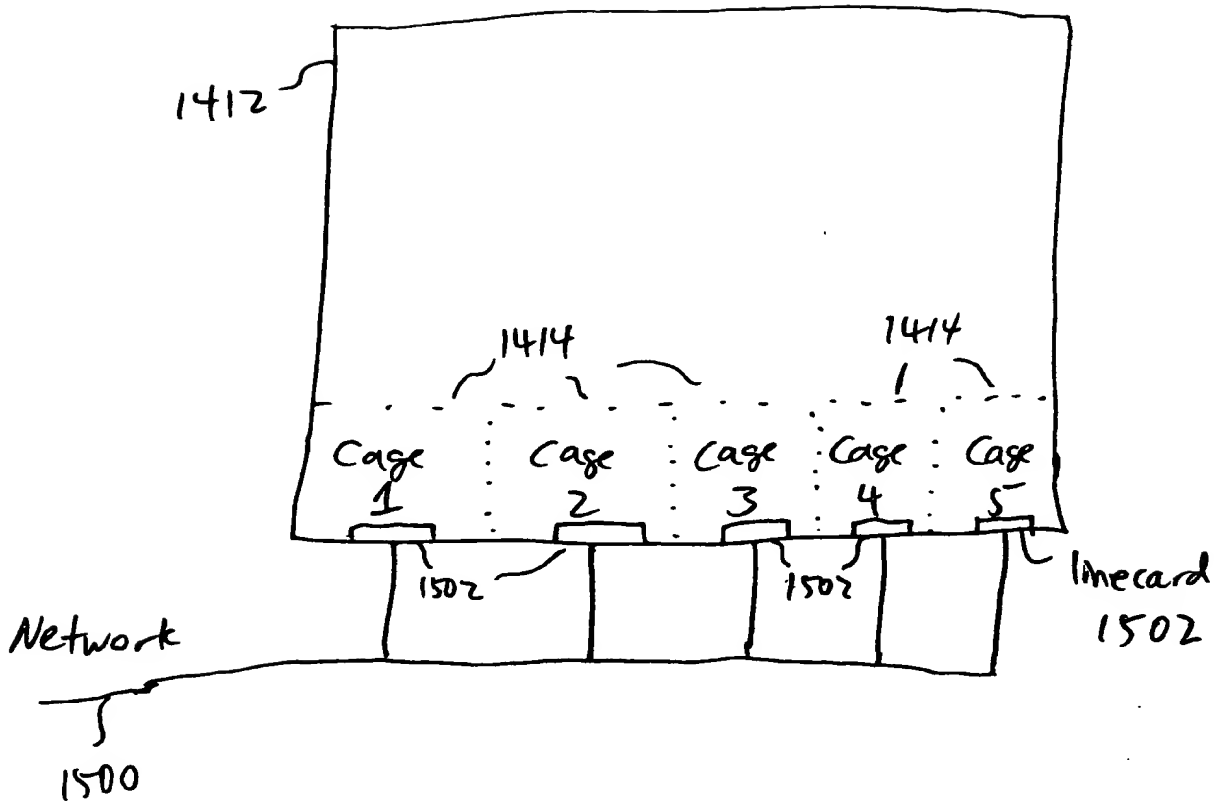


Figure 15

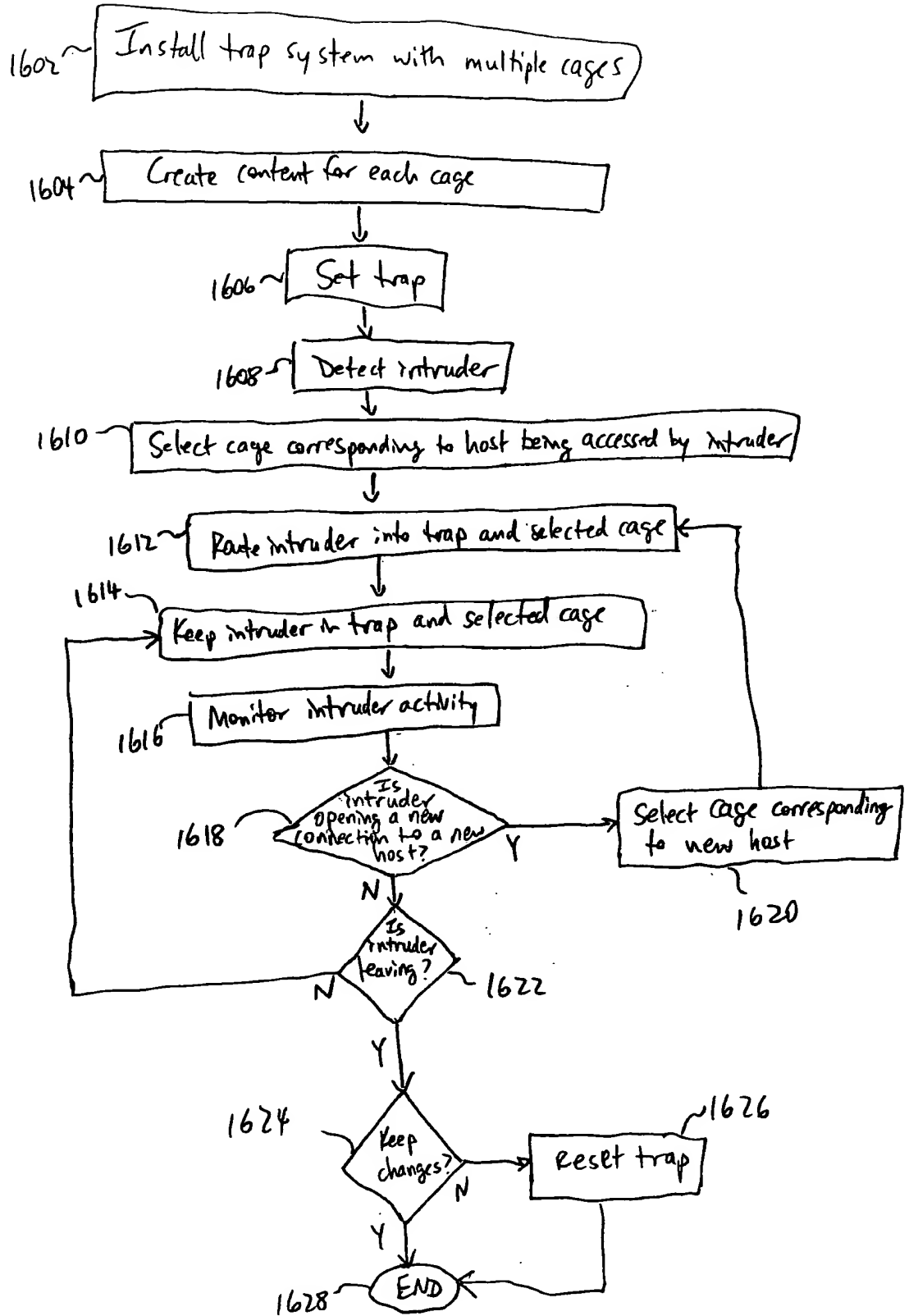
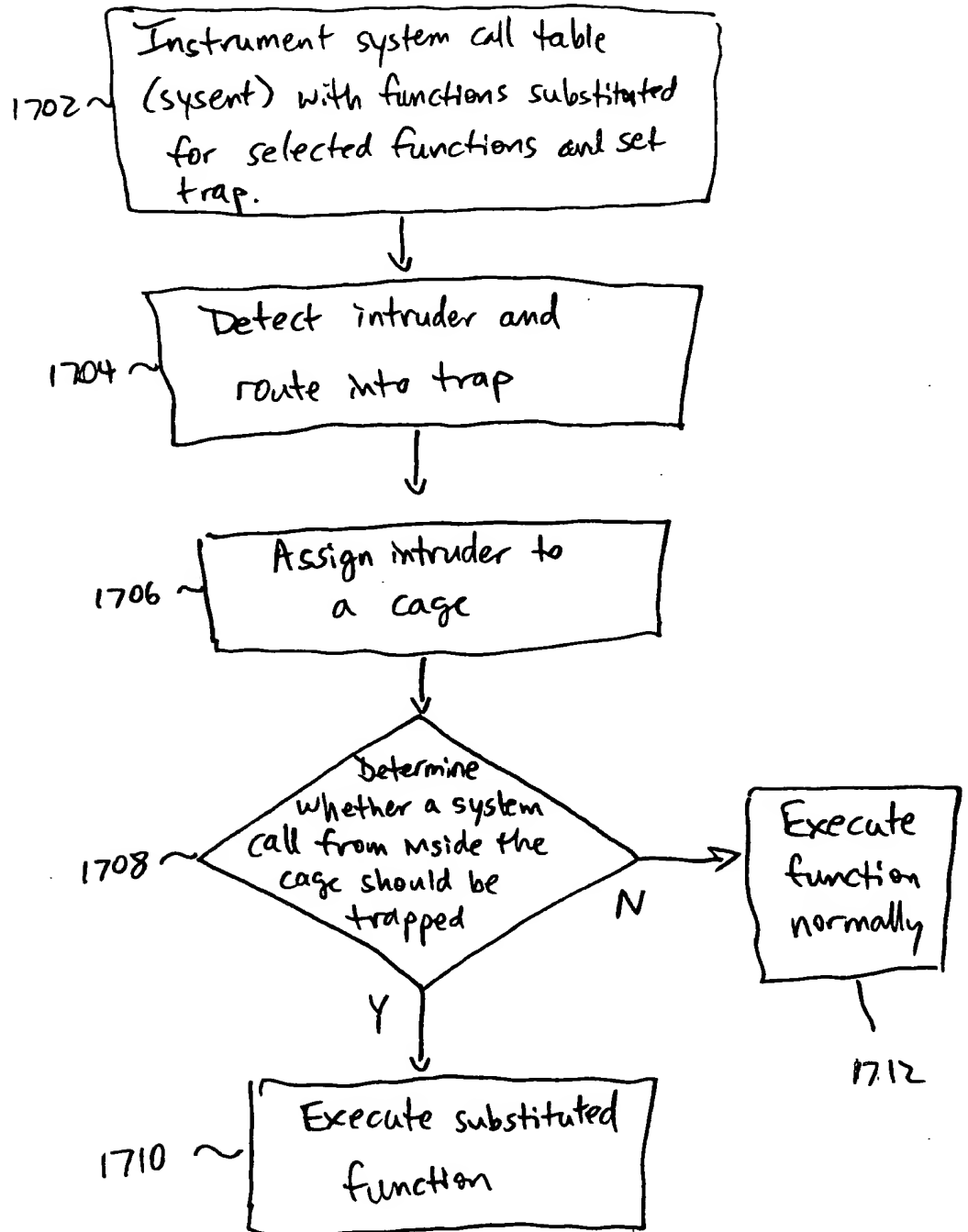


FIGURE 16

09841700:072701



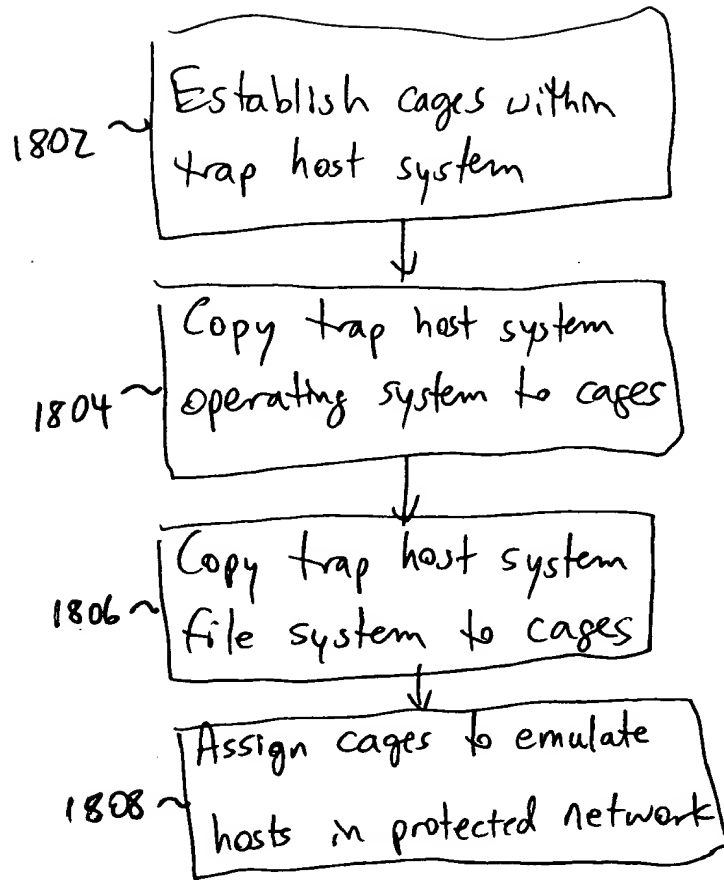


Figure 18

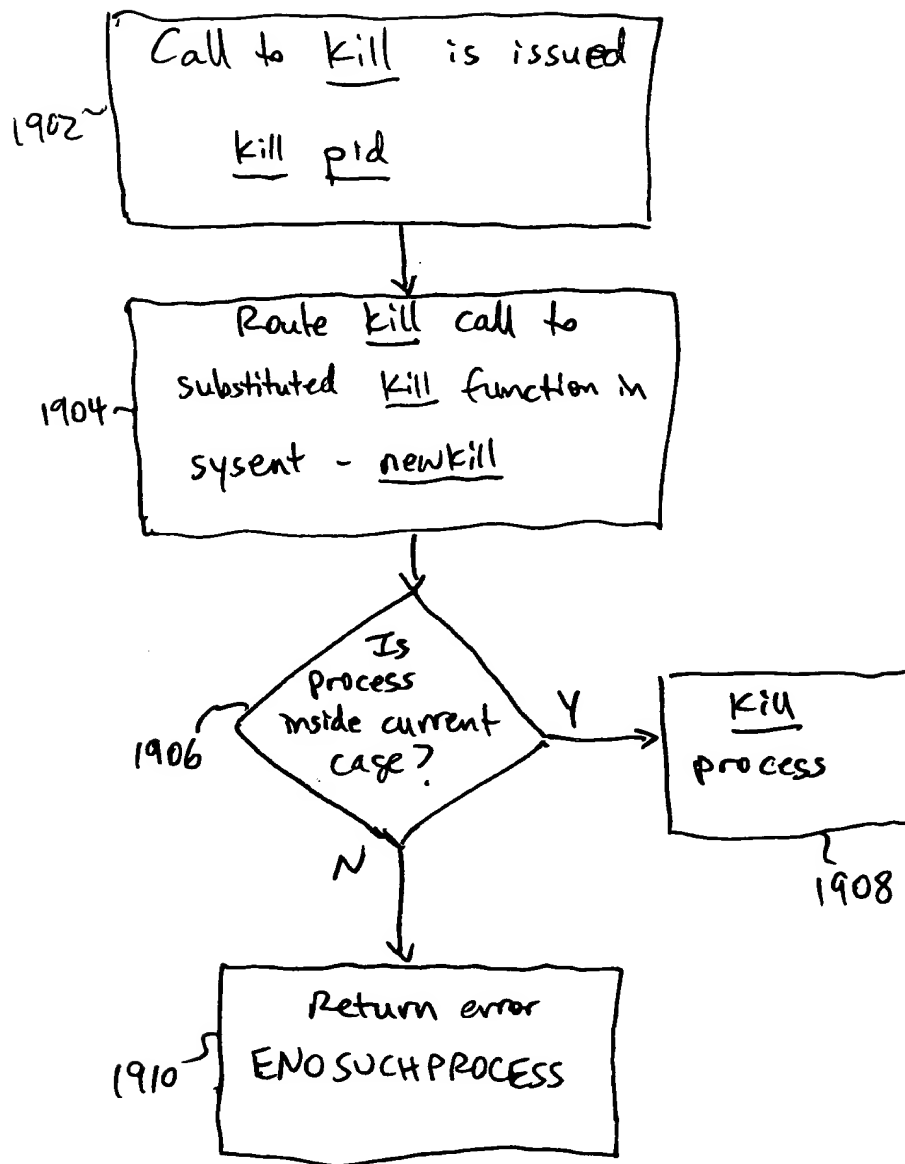


Figure 19

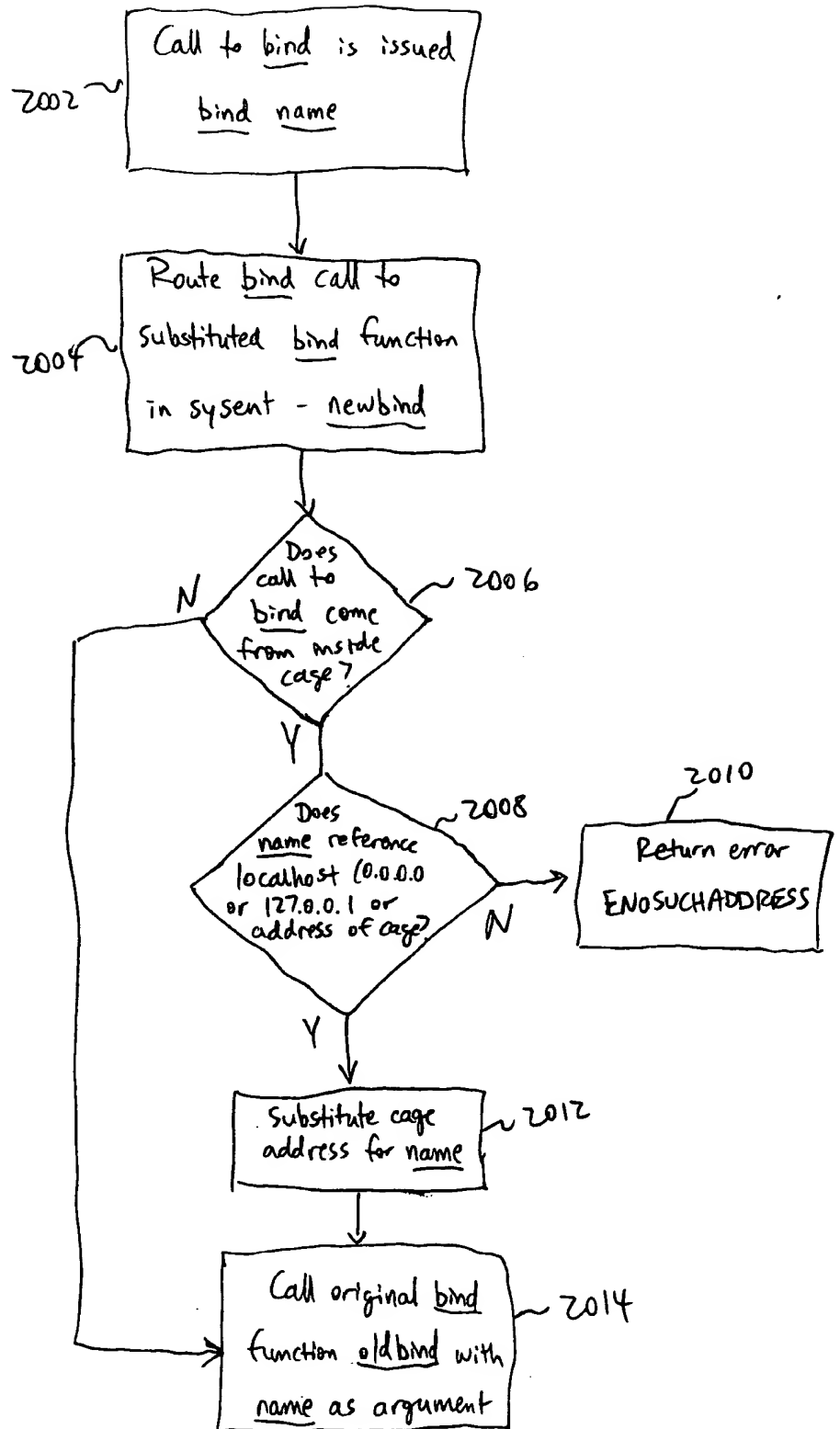


Figure 20

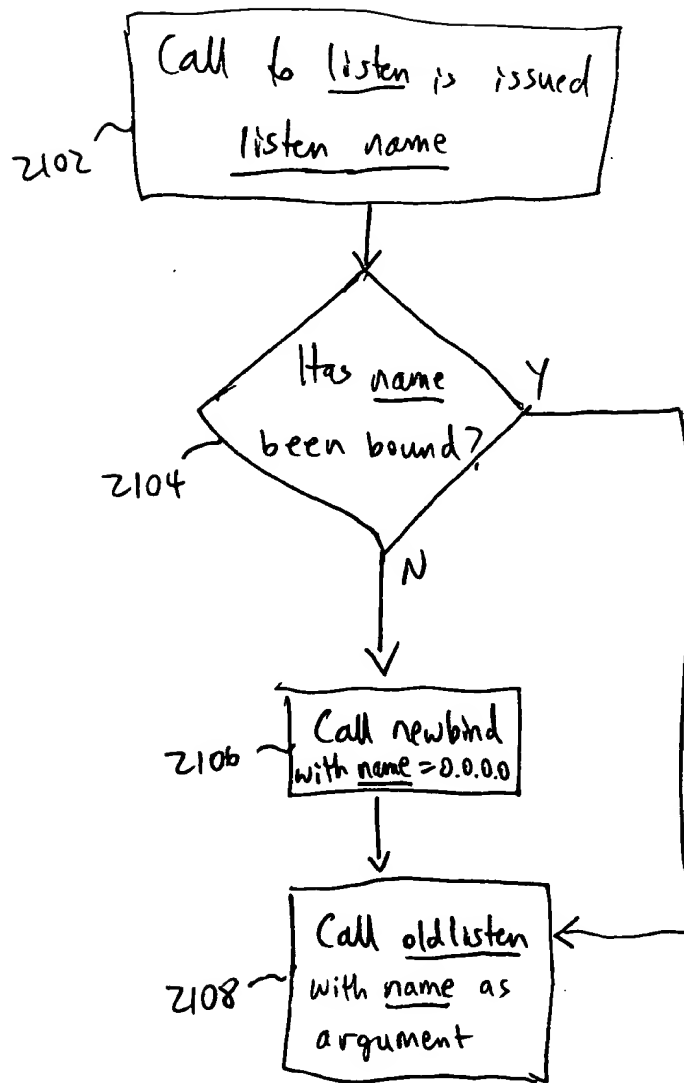


Figure 21

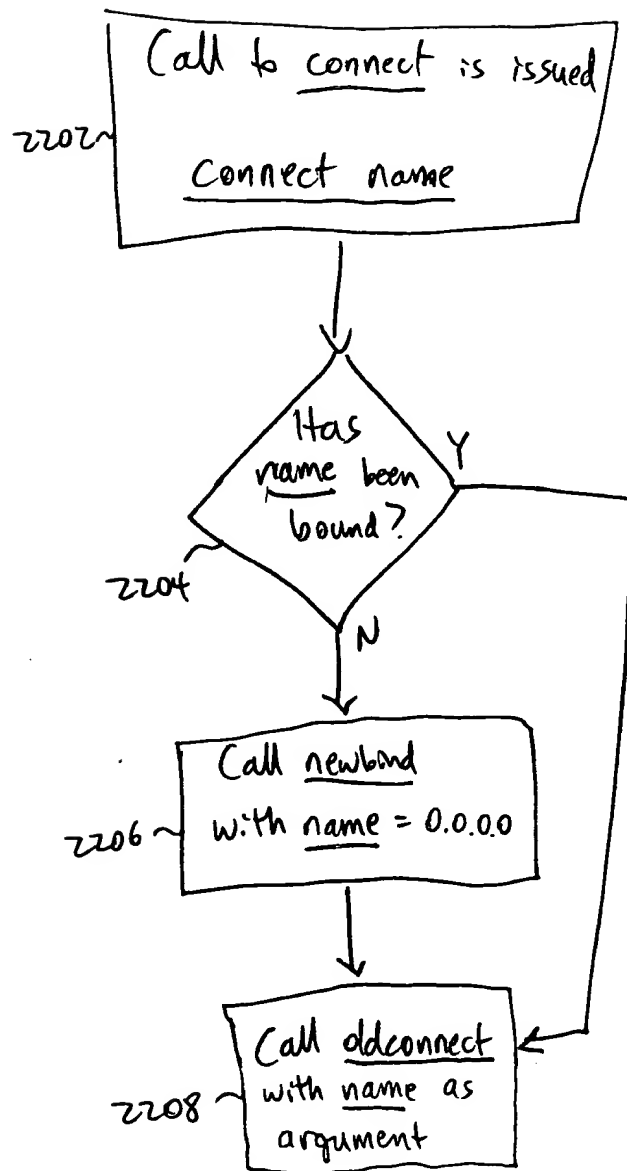


Figure 22



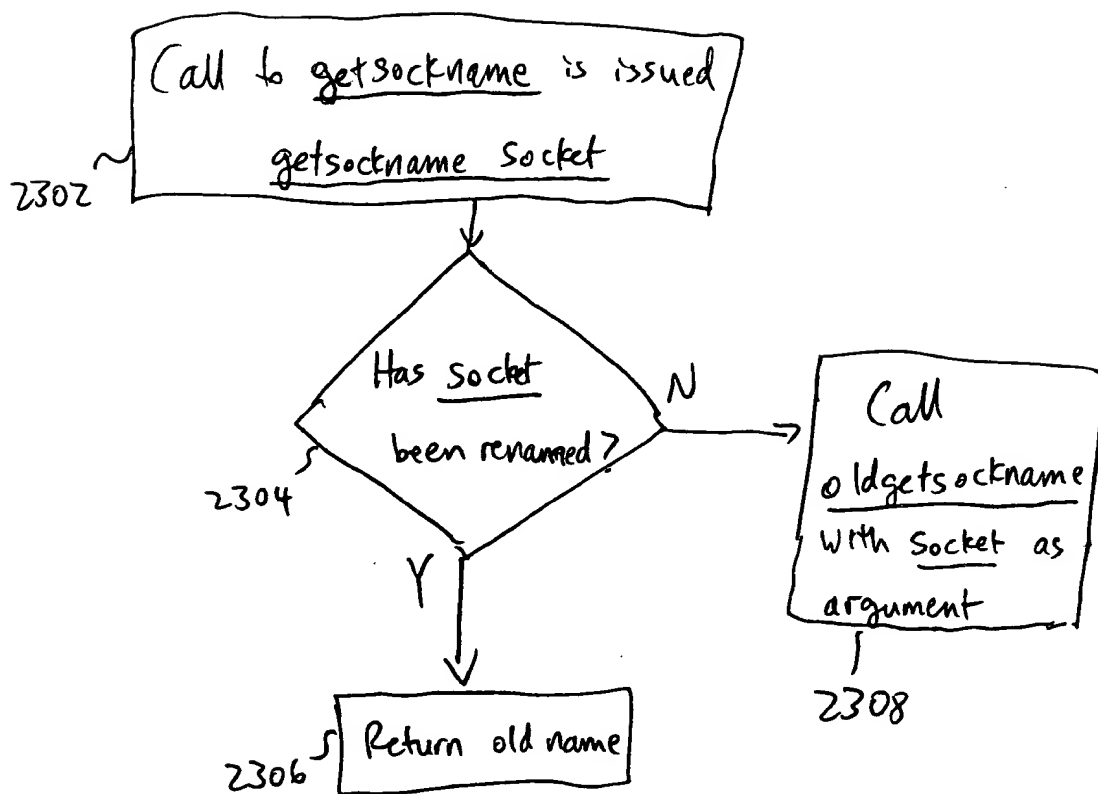


Figure 23

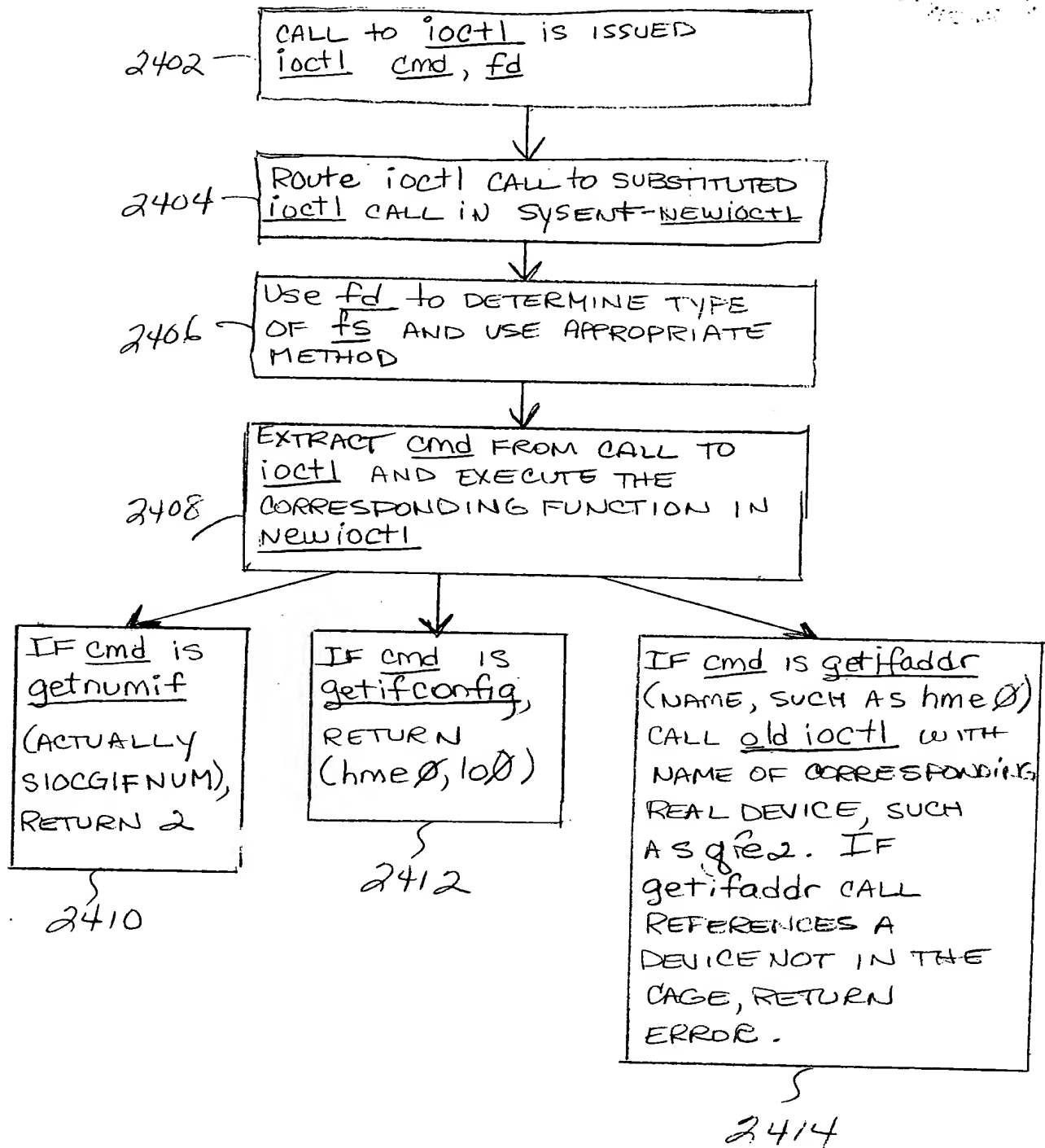


FIGURE 24

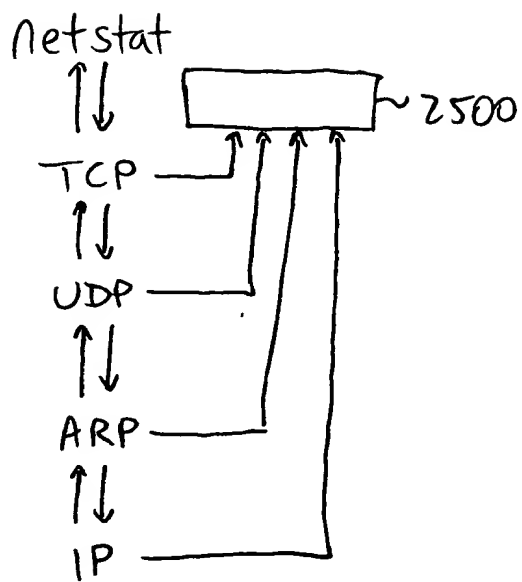


Figure 25

```

<doc>
<regexp-query>
  <name>Possible SGID Exploit</name>
  <properties>
    <priority>10</priority>
  </properties>
  <pattern>
    <next>
      <line>.*exec args=.*pid=\((\d+)\); ppid=\((\d+)\); uid=\((\d+)\); euid=
        \((\d+)\); gid=\([1-9]\d*\); egid=\(0\).*</line>
    </next>
    <next>
      <line>.*args=\([^\-\\w\\\/ ]+\); pid=\((\d+)\); ppid=\(%1%\).*</line>
    </next>
  </pattern>
  <procmatch>
    <actionpair>
      <line>.*args=\([^\-\\w\\\/ ]+\).*ppid=\(%1%\).*</line>
      <action>
        <highlight/>
        <delete/>
        <varop var="agg">%1%</varop>
      </action>
    </actionpair>
  </procmatch>
  <annotation>
    <text>Possible SGID Exploit: %agg%</text>
  </annotation>
</regexp-query>
</doc>

```

Figure 26

```

<doc>
  <regexp-query>
    <name>Possible SUID Exploit</name>
    <properties>
      <priority>10< /priority>
    </properties>
    <pattern>
      <next>
        <line>.*exec args=.*pid=\((\d+)\); ppid=\(\d+\); uid=\([1-9]\d*\);
euid=\(0\).*</line>
      </next>
      <next>
        <line>.*args=\(.+\); pid=\(\d+\); ppid=\(%1%\).*</line>
      </next>
    </pattern>
    <procmatch>
      <actionpair>
        <line>.*args=\(.+\); pid=\(\d+\); ppid=\(%1%\).*</line>
        <action>
          <highlight/>
          <delete/>
          <varop var="agg">%1%</varop>
        </action>
      </procmatch>
      <annotation>
        <text>Possible SUID Exploit: %agg%</text>
      </annotation>
    </regexp-query>
  </doc>

```

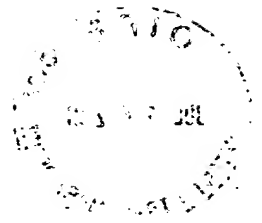
Figure 27

09841700-072701

<doc>  
<regexp-query>  
 <name>All Processes</name>  
 <properties>  
 <priority>10</priority>  
 </properties>  
 <pattern>  
 <next>  
 <line>.\*proclog.\*args=\(((\\-\\.\\w\\\\/ ]+))\\).\*</line>  
 </next>  
 </pattern>  
 <procmatch>  
 <actionpair>  
 <line>.\*args=\(((\\-\\.\\w\\\\/ ]+))\\).\*</line>  
 <action>  
 <highlight/>  
 <delete/>  
 <varop var="agg">%1%</varop>  
 </action>  
 </actionpair>  
 </procmatch>  
 <annotation>  
 <text>Process started: %agg%</text>  
 </annotation>  
</regexp-query>  
</doc>

Figure 28

09841700:072701



```
<doc>
<regexp-query>
  <name>Find Processes...</name>
  <properties>
    <priority>10</priority>
  </properties>
  <args>
    <args>.+</args>
    <pid>\d+</pid>
    <ppid>\d+</ppid>
    <uid>\d+</uid>
    <euid>\d+</euid>
    <gid>\d+</gid>
    <egid>\d+</egid>
  </args>
  <pattern>
    <next>
      <line>.*args=\(%args%\); pid=\(%pid%\); ppid=\(%ppid%\);
uid=\(%uid%\); euid=\(%euid%\); gid=\(%gid%\); egid=\(%egid%\).*</line>
    </next>
  </pattern>
  <procmatch>
    <actionpair>
      <line>.*args=\(.*\%\); pid.*</line>
      <action>
        <highlight/>
        <delete/>
        <varop var="agg">%1%</varop>
      </action>
    </actionpair>
  </procmatch>
  <annotation>
    <text>Process started: %agg%</text>
  </annotation>
</regexp-query>
</doc>
```

Figure 29

09841700.072701

```
<doc>
<regexp-query>
  <name>All Shell-spawned Processes</name>
  <properties>
    <priority>l0</priority>
  </properties>
  <pattern>
    <next>
      <line>.*exec args=\(-sh\); pid=\(((d+)\)).*</line>
    </next>
    <next>
      <line>.*args=\(((\[-\w\\\/ ]+)\)).*ppid=\(%l%\).*</line>
    </next>
  </pattern>
  <procmatch>
    <actionpair>
      <line>.*args=\(((\[-\w\\\/ ]+)\)).*ppid=\(%l%\).*</line>
      <action>
        <highlight/>
        <varop var="agg">%l%</varop>
      </action>
    </actionpair>
  </procmatch>
  <annotation>
    <text>Executed from a shell: %agg%</text>
  </annotation>
</regexp-query>
</doc>
```

Figure 30



09641700.072704

```
<doc>
<regexp-query>
  <name>Incoming Connections</name>
  <properties>
    <priority>l0</priority>
  </properties>
  <pattern>
    <next>
      <line>.*incoming connection from=\(.+\).*</line>
    </next>
  </pattern>
  <procmatch>
    <actionpair>
      <line>.*incoming connection from=\((.+):(.+)\)</line>
      to=\((.+):(.+)\).*</line>
      <action>
        <highlight/>
        <delete/>
        <varop var= "fromip">%1%</varop>
        <varop var= "fromport">%2%</varop>
        <varop var= "toip">%3%</varop>
        <varop var= "toport">%4%</varop>
      </action>
    </actionpair>
  </procmatch>
  <annotation>
    <text>Incoming Connection From IP: %fromip% (on port: %fromport%) To
    IP: %toip% (on port: %toport%)</text>
  </annotation>
</regexp-query>
</doc>
```

Figure 31

09641700 072704

```
<doc>
<regexp-query>
  <name>Keystrokes Entered</name>
  <properties>
    <priority>10</priority>
  </properties>
  <pattern>
    <next>
      <line>.*read stream data, id=\((\d+)\) data=\(.+\).*</line>
    </next>
    <next fromprev="1">
      <line>.*read stream data, id=\(%1%\) data=\(.*\0[ad4].*\).*</line>
    </next>
  </pattern>
  <procmatch>
    <actionpair>
      <line>.*read stream data, id=\(%1%\) data=\(.+\).*</line>
      <action>
        <highlight/>
        <delete/>
        <varop var="agg">%1%</varop>
      </action>
    </actionpair>
  </procmatch>
  <annotation>
    <text>Keystrokes Entered: %agg%</text>
  </annotation>
</regexp-query>
</doc>
```

Figure 32

09841700.072704

<doc>  
<regexp-query>  
 <name>Screen Output</name>  
 <properties>  
 <priority>10</priority>  
 </properties>  
 <pattern>  
 <next>  
 <line>.\*write stream data, id=\(((\d+)\)) data=\((.+)\).\*</line>  
 </next>  
 <next fromprev="1">  
 <line>.\*write stream data, id=\(%1%\)  
data=\(.\*\0[ad46].\*\).\*</line>  
 </next>  
 </pattern>  
 <procmatch>  
 <actionpair>  
 <line>.\*write stream data, id=\(%1%\) data=\(((.+)\))).\*</line>  
 <action>  
 <highlight/>  
 <delete/>  
 <varop var="agg">%1%</varop>  
 </action>  
 </actionpair>  
 </procmatch>  
 <annotation>  
 <text>Output to screen: %agg%</text>  
 </annotation>  
</regexp-query>  
</doc>

Figure 33

09841700.072704

```
<doc>
<regexp-query>
  <name>Find Monitored</name>
  <properties>
    <priority>10</priority>
  </properties>
  <args>
    <file_name>.+</file_name>
    <pid>\d+</pid>
  </args>
  <pattern>
    <next>
      <line>.*monitored file opened name=\(%file_name%\)
pid=\(%pid%\).*</line>
    </next>
    </pattern>
    <procmatch>
      <actionpair>
        <line>.*monitored file opened name=\((.+)\)
pid=\((.+)\).*</line>
        <action>
          <highlight/>
          <delete/>
          <varop var="filename">%1</varop>
          <varop var="pidvar">%2</varop>
        </action>
      </actionpair>
    </procmatch>
    <annotation>
      <text>File Opened: %filename% (from pid: %pidvar%)</text>
    </annotation>
  </regexp-query>
</doc>
```

Figure 34